DRMS Instruction 5200.1

DRMS-IZ

14 May 96

PROCESSING OF REQUESTS FOR COMPUTER USER ACCOUNTS
(Supplementation is prohibited)

A. REFERENCES.

1. DRMS-R 5200.1, Processing of Requests For Computer User Accounts, 4 May 93, superseded.

2. DLAR 5200.17, Security Requirements For Automated Information and Telecommunications Systems.

3. DRMS-M 5210.1, TASO Manual, Guidelines and Procedures For TASO (Terminal Area Security Officer).

4. Automated Usercode Request Application (AURA) User's Documentation.

5. DoD Directive 5200.28, Security Requirements For Automated Information Systems.

6. DRMS Directive 5200.1, Processing of Requests for Computer User Accounts.

B. PURPOSE. This instruction provides guidance in taking add, change or delete actions on user access capabilities for all DLA/DRMS computer systems. It standardizes specific actions and required documentation for all locations.

C. APPLICABILITY.

1. This instruction applies to all Offices/Directorates of HQ DRMS and all DRMS field activities.

2. DLA has implemented a policy of assigning one standard logon identifier to each person who requires access to a DLA computer system, and that person will have only one standard logon identifier for access to any/all computer systems or applications. This is referred to as the 'DLA STANDARD LOGON ID'.

D. DEFINITIONS.

1. Audit. An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures.

2. AURA. The Automated User Request Application System is designed to help people gain access to any of the computer systems in DRMS quickly and conveniently. It reduces paper handling, improves security control and makes it easier for the people who administer the computer systems to collect the information they need.

3. Authenticate. To establish the validity of a claimed identity.

4. Data Owner. The individual(s) responsible for making decisions regarding the protection and use of sensitive information. For AISs, data owners are the persons responsible for the business functions supported by the AISs.

5. Information System Security Officer (ISSO). The activity focal point for all computer security matters. In his/her operational capacity, the ISSO implements the provisions of DLAR 5200.17 and develops local security procedures for the administration of the activity computer security program. The ISSO oversees user account administration, manages the TASO program and reports possible security violations.

6. Terminal Area Security Officer (TASO). The activity focal point for all local office and terminal security matters. TASOs serve as the initial security contact point for the users in their office areas. TASOs assist the ISSO to assure compliance with security procedures in an assigned area, and implement security requirements fo remote devices and terminals. TASOs report security incidents and violations to the ISSO. TASOs conduct security awareness training.

7. Users. People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by responsible individual).

E. PROCEDURES.

1. Initial Access Request.

a. The user contacts his/her TASO to inform the TASO of the need for access to a computer system resource or application.
b. The user and the TASO discuss the specifics of the needed access.
c. The user provides detailed information to the TASO.

2. Forms Composition.

a. The TASO refers to the AURA Users Guide for assistance.
b. The TASO accesses AURA and fills out the forms needed for the computer system access.

3. Forms Submittal.

a. When the TASO completes the AURA access, the completed forms are forwarded to the user’s supervisor in accordance with the instructions in the AURA Users Guide.
b. The supervisor reviews the employee’s initial request and makes the decision regarding whether the request is appropriate. The supervisor will either approve or disapprove the request.
c. If the supervisor approves the request, the supervisor will forward the AURA form to the appropriate data owner(s) as specified in the e-mail instructions.
d. If the supervisor disapproves the request, the supervisor informs the TASO who originated the request.

4. System and Data Access Approvals.

a. The data owner receives the access request that has been submitted by the requesting supervisor.
b. The data owner reviews the forms to determine the propriety of requested accesses and privileges.

c. If the data owner denies the request, the form will be returned to the supervisor with an explanation.
d. If the data owner approves the request, the data owner refers to the e-mail instructions to determine the appropriated personnel who will establish the system accesses and privileges.

5. Processing of Data Owners Approved Requests.

a. The ISSO, System Monitor, or Administrator receives the AURA form from the data owner.
b. The appropriate personnel take the action to establish the accesses and privileges.
c. The appropriate personnel notify the user of the established access according to enclosure 1.

6. User Notification.

a. The user receives the notification form (enclosure 1).
b. The user signs the appropriate receipts.
c. The user sends one receipt to the ISSO/System Monitor and one receipt to his/her TASO.

7. Documentation and Record Keeping. The ISSO/TASO store AURA access request records and password receipts and retain them indefinitely.

F. RESPONSIBILITIES.

1. The Director, Office of Command Security, (DRMS-I), will administer the entire ADP Computer Security Program, develop directives and instructions and provide guidance.

2. The ISSO, ADP Computer Security Administration Division, (DRMS-IZ), will:

a. Be responsible for account adjustments on all computer systems located at HQ DRMS.
b. Receive and act on all requests involving access to HQ DRMS computer systems.
c. Maintain a file of all appointed Terminal Area Security Officers located throughout HQ DRMS and all DRMS field activities.
d. Assure access records are audited and reviewed.

3. The commanders, directors and chief (DRMS HQ and all DRMS field activities) will:

a. Appoint TASOs.
b. Assure TASOs refer to DRMS-M 5210.1 and adhere to its guidelines and policies.
c. Assure that TASOs follow ADP security regulations and follow proper security procedures in accomplishing their responsibilities.
d. Assure that TASOs use the AURA system in processing new user requests, changes and deletions to all DRMS Systems.

4. Supervisors will:

a. Approve a user’s initial request for system access.
b. Initiate user delete actions when appropriate.

5. TASOs will:

a. Process add, change and delete actions within 24 hours of receiving the request.
b. Determine if the user already has a DLA standard Logon identifier assigned, and whether the identifier is appropriate for access to the requested system.
c. Ensure that only standard logon identifiers are employed for user access.

6. The users will:

a. Provide all pertinent information to the TASOs when requesting system access.
b. Be responsible for providing accurate data.
c. Be required to sign and return receipts upon receiving notification of their standard logon identifier and password.

7. Data owners will take timely action to either approve or deny requests for access to data. If the data owner denies the access, he/she will advise the requester of the reason access is being denied.

8. ISSOs, System Monitors and Administrators take approved forms and establish the requested access capabilities and privileges.

G. EFFECTIVE DATE AND IMPLEMENTATION. This instruction is effective upon its publication.

H. INFORMATION REQUIREMENTS. (Reserved for future use.)

BY ORDER OF THE COMMANDER

/s/
STEVEN P. HOCKETT
Colonel, USAF
Deputy Commander

1 Encl
Notification of
Computer Access

Encl 1
DRMS Instruction 5200.1

<put your letter head>

SUBJECT: Standard Logon Identifier/Password Assignment

1. The following information provides you access to the system and files indicated below. If you experience difficulties logging onto the system contact your TASO for assistance.

2. Standard Logon Identifier assignment: _____

Password: ____#_____(see TASO for gaining access)

System(s): _____

Telnet Address for each systems: _____

3. Guidelines are enclosed. Please complete and return the receipts below. Any further questions should be directed to your TASO.

_____

_____

Store Manager

DRMO-_____

YOU ARE REQUIRED TO IMMEDIATELY CHANGE YOUR PASSWORD AFTER SIGNING ONTO THE SYSTEM WITH YOUR STARTER PASSWORD THAT HAS BEEN ASSIGNED TO YOU. NOTE: IRIS USERS DO NOT CHANGE YOUR PASSWORDS.

**********RETURN TO ISSO OR SYSTEM MONITOR WHO ASSIGNED ACCESS.**********

SUBJECT: Standard Logon Identifier/Password assignment for the following system(s): _____

TO: _____

_____

_____

I hereby acknowledge receipt of my standard logon identifier/password. I have read the enclosed instructions of my responsibilities.

(Please print your name and Office Symbol: _____

DATE: _____ Signature: _____

Userid: _____

Enclosure 1
DRMS Instruction 5200.1

ADP Security Instructions

1. Employee Responsibility:

As a user of a U.S. Government ADP system, you are responsible for the security of the systems and data you access. You must immediately change your password after signing on with your starter password. Please sign and return the enclosed receipts as soon as possible.

2. Computer Equipment:

a. **DON'T** take computer equipment or materials home with you.

b. **DON'T** bring privately owned hardware/software to work.

c. **DON'T** make copies of copyrighted software.

d. If you leave a terminal or computer even for a short time, you must sign off. This to be the most serious violation in that it leaves the system open for intrusion. It is you responsibility to make sure that the terminal you use is secured.

e. Personal use of a terminal or desktop computer is forbidden including for personal transactions, storing personal information, sending personal messages, and playing games. Personal use of government computer is punishable under both Federal statute and DLA regulation. DO NOT DO IT!

3. Passwords:

a. **Do Not** let anyone use your standard logon identifier/password. No sharing allowed.

b. Use 6 to 8 ALPHA-NUMERIC characters for your password, & at least one embedded numeric.

c. Your standard logon identifier is assigned to you. No one else will be issued this logon identifier.

d. Change your password periodically, you don't have to wait for the 90 day limit to be up.

e. Most systems are now keeping history records of password used and do not allow for the reuse of previous passwords.

f. **DON'T** write your password down or discuss it.

g. **DON'T** inform anyone of your password. This includes your supervisor, fellow employee, etc.

h. If you forget your password, inform your TASO immediately if one is assigned to your area. If there is not a TASO contact the HQ DRMS Information System Security Officer (ISSO) at DSN 932-4217 or DSN 932-7013.

4. Violations

Report **ALL** violations of security procedures to your TASO, the ISSO, or the System Security Administrator. Violations include, but are not limited to, the following:

a. Compromise of a password.

b. Unauthorized attempts to access a computer, programs, data or information.

c. Failure to sign off of the computer.

d. Using computer for personal use.